

REMARKS

Claims 5, 10, 22 have been amended to correct obvious typographical error and an informality. Accordingly, all claim amendments herein are directed towards matters of form and thus are unrelated to patentability.

Applicant has also amended the description to correct an obvious typographical error.

The headings below are numbered to correspond with the heading numbering used by the Examiner in the Office Action.

3. The informality of Claim 22 has been corrected.

Claim 22 has been amended to recite "The method of claim 11" at line 1. Accordingly, the informality noted by the Examiner has been corrected.

For the above reason, Applicant respectfully requests reconsideration and withdrawal of the objection to Claim 22.

4. Claims 1-3, 6-8, 13-15, 17-20, and 21 are patentable over Houston et al. (2002/0019945) in view of Blakely-Fogel et al. (4,864,492).

As to Houston et al., the Examiner admits:

Houston doesn't teach that adding knowledge to the common format event using knowledge base table files to generate a knowledge-containing common format event. (Office Action, page 3.)

Blakely-Fogel et al. does not cure this glaring deficiency in Houston et al. With regards to Blakely-Fogel et al., the Examiner states:

However, Blakely-Fogel teaches that adding knowledge (i.e. modifying or changing) to the common format event using knowledge base table files [Fig. 2] to generate a knowledge-containing common format event [Fig. 2 "Knowledge base table", Fig. 3 "change current data"]. (Office action, page 3, emphasis in original.)

The Examiner's statement is respectfully traversed. Blakely-Fogel et al. teaches (1) the knowledge base comprises rules; (2) that if the user's input conforms to the rules then **the user's input becomes the current data in the current database**; and (3) that if the user's input does not conform to the rules, **the rule** the user needs to correct the error of the user's input **is displayed to the user**. Thus, the Examiner has failed to callout where Blakely-Fogel et al. teaches or suggests "adding knowledge (i.e. modifying or changing) **to the common format event** using knowledge base table files" as asserted by the Examiner, emphasis added.

Specifically, Blakely-Fogel et al. teaches (1) the knowledge base comprises rules:

**The knowledge base 20 comprises rules 21 as shown in FIG. 2.** The rules 21 contain expert knowledge about the network architecture and the network architecture adapters that are supported by the particular network architecture such as SNA. For example, a rule 21 may cover the type of information being supplied, such as whether the information supplied is a connection name. If it is a connection name, a rule will cover the allowable names a user may select. The rules may state which characters can comprise an allowable name. The rule might state that connection names can only comprise the letters between capital A and Capital Z, an asterisk \*, and the dollar sign \$. (Col. 3, lines 63 to col. 4, line 7, emphasis added.)

Further, Blakely-Fogel et al. teaches (2) that if the user's input conforms to the rules then the user's input becomes the current data in the current database:

If the user's input conforms to the rules 21 of the network architecture, **then the user's input becomes the current data in the current data base 50** as it resides in I/O storage device 6 of 50 is referenced by field G of the reference pointers 23 of a knowledge rule 21. **The user's input replaces the data previously residing in the current data base 50.** (Col. 4, line 64 to col. 5, line 2, emphasis added.)

Finally, Blakely-Fogel et al. teaches (3) that if the user's input does not conform to the rules, the rule the user needs to correct the error of the user's input is displayed to the user:

**If the user's input does not conform to the rules 21 of the network architecture, then the control 30 accesses the user interface 40 to display to the user the rule 21 the user needs to correct the error of the user's previous input, step 35. (Col. 5, lines 2 to line 6, emphasis added.)**

Further, Applicant respectfully submits the Examiner has failed to make a prima facie obviousness rejection. Applicant notes that to make a prima facie obviousness rejection, the MPEP directs:

**BASIC CONSIDERATIONS WHICH APPLY TO OBVIOUSNESS REJECTIONS**

When applying 35 U.S.C. 103, the following tenets of patent law must be adhered to:

- (A) The claimed invention must be considered as a whole;
- (B) The references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination;
- (C) The references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention; and
- (D) Reasonable expectation of success is the standard with which obviousness is determined.

MPEP § 2141, Rev. 3, August 2005, p. 2100-125. It is noted that this directive stated "the following tenets . . . must be adhered to." Accordingly, failure to adhere to any one of these tenets means that a prima facie obviousness rejection has not been made.

The rejection fails to adhere to multiple of these tenets.

As demonstrated more completely below, the references have not been considered as a whole and the references do not suggest the desirability of making the combination. Pieces of the references have been extracted and selectively interpreted in view of Applicant's claims. Finally, there is no explanation

of how the primary reference would work for its intended purpose following the modification.

Initially, Applicant notes that Blakely-Fogel et al. teaches:

This invention relates to ... **configuring a system in accordance with the protocol of the network architecture while providing the user with feedback indicative of problems associated with an invalid request** to facilitate a valid user entry. (Col. 1, lines 7-11, emphasis added.)

Thus, instead of considering Blakely-Fogel et al. as a whole as teaching configuring a system in accordance with the protocol of the network architecture while providing the user with feedback indicative of problems associated with an invalid request, the Examiner has extracted the term "knowledge base table" from Blakely-Fogel et al. and selectively interpreted the term in view of Applicant's claimed invention.

The support the Examiner provides for the Examiner's assertion the Blakely-Fogel et al. teaches "adding knowledge (i.e. modifying or changing) to the common format event using knowledge base table files" is "[**Fig. 2 "Knowledge base table", Fig. 3 "change current data"**]", emphasis in original.

However, as discussed above, the "knowledge base table" contains rules, the rules containing expert knowledge about the network architecture and the network architecture adapters. As also discussed above, the "change current data" occurs when the user's input becomes the current data in the current data base.

Thus considering Blakely-Fogel et al. as a whole, the Examiner has failed to callout how Blakely-Fogel et al. has anything to do with a common format event or security events in general.

For similar reasons, the Examiner has failed to callout where Houston et al., Blakely-Fogel et al., either alone or in combination, suggest the desirability or obviousness of the combination. Applicant respectfully submits the Examiner is

using hindsight reconstruction to deprecate Applicant's claimed invention.

For at least the above reasons, Houston et al. in view of Blakely-Fogel et al. does not teach or suggest:

A method of producing at least one alert indication based on a number of events derived from an enterprise comprising:

providing a plurality of enterprise device outputs, at least a portion of the outputs having different formats, each output containing an event relating to an enterprise device;

translating each output into a common format event,

**adding knowledge to the common format event using knowledge base table files to generate a knowledge-containing common format event;** and

applying one or more rules from a set of rules to the knowledge-containing common format event to generate the alert indication,

as recited in Claim 1, emphasis added. Accordingly, Claim 1 is allowable Houston et al. in view of Blakely-Fogel et al. Claims 2-3, 6-8, 13-14, 21, which depend from Claim 1, are allowable for at least the same reasons as Claim 1.

For similar reasons, Houston et al. in view of Blakely-Fogel et al. does not teach or suggest:

A system for producing at least one alert indication based on a number of events derived from an enterprise comprising:

a plurality of enterprise devices, each device capable of producing an output;

a number of translation files, the translation files allowing the output to be translated into a common format event;

a number of knowledge base table files, matching of the common format event with one or more of the knowledge base table files **adding knowledge from the matched file** to generate a knowledge-containing common format event;

a number of rule files, the rule files governing generation of the alert indication,

as recited in Claim 15, emphasis added. Accordingly, Claim 15 is allowable over Houston et al. in view of Blakely-Fogel et al. Claims 17-20, which depend from Claim 15, are allowable for at least the same reasons as Claim 15.

For the above reasons, Applicant respectfully requests reconsideration and withdrawal of this rejection.

5. Claims 4, 9, and 16 are patentable over Houston et al. in view of Blakely-Fogel et al. and further in view of Lim (2004/0250133).

As set forth above, Claims 1, 15 are allowable over Houston et al. in view of Blakely-Fogel et al. Claims 4, 9 and Claim 16, which depend from Claim 1 and Claim 15, respectively, are allowable over Houston et al. in view of Blakely-Fogel et al. for at least the same reasons as Claim 1 and Claim 15. The Examiner has failed to callout where Lim cures the previously described deficiencies in Houston et al. in view of Blakely-Fogel et al. Accordingly, Claims 4, 9 and 16 are allowable over Houston et al. in view of Blakely-Fogel et al. and further in view of Lim.

For the above reasons, Applicant respectfully requests reconsideration and withdrawal of this rejection.

6. The Objection to Claims 5, 10-12, 22 should be withdrawn.

As set forth above, Claim 1 is allowable. Claims 5, 10-12, 22, which depend from Claim 1, are allowable for at least the same reasons as Claim 1.

For the above reason, Applicant respectfully requests reconsideration and withdrawal of the objection to Claims 5, 10-12, 22.

#### CONCLUSION

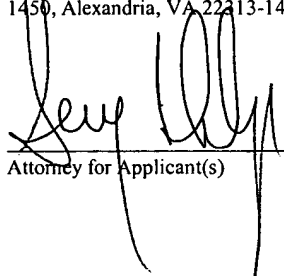
Claims 1-22 are pending in the application. For the foregoing reasons, Applicant respectfully requests allowance of all pending claims. If the Examiner has any questions relating

Appl. No. 10/080,574  
Amdt. dated October 20, 2005  
Reply to Office Action of July 27, 2005

to the above, the Examiner is respectfully requested to  
telephone the undersigned Attorney for Applicant(s).

**CERTIFICATE OF MAILING**

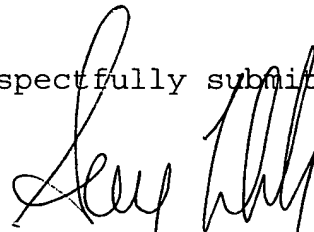
I hereby certify that this correspondence is being deposited with the  
United States Postal Service with sufficient postage as first class mail  
in an envelope addressed to: Commissioner for Patents, P.O. Box  
1450, Alexandria, VA 22313-1450, on October 20, 2005.



Attorney for Applicant(s)

October 20, 2005  
Date of Signature

Respectfully submitted,



Serge J. Hodgson  
Attorney for Applicant(s)  
Reg. No. 40,017  
Tel.: (831) 655-0880